Identificação de Endereços IP Dinâmicos com Dados Públicos

Gabriel Pains de Oliveira Cardoso[1] **Leonardo B. Oliveira**[1] **Ítalo Cunha**[1]

[1] Departamento de Ciência da Computação — Universidade Federal de Minas Gerais

{gabriel.cardoso,leob,cunha}@dcc.ufmg.br

Abstract. *We introduce DynMap, a system to identify dynamically-assigned IP addresses. DynMap tracks hosts using publicly-accessible HTTPS certificate fingerprints, making DynMap generally applicable by any network operator. We develop mechanisms to deal with HTTPS certificate sharing across multiple devices as well as reverse proxies and load balancers. We apply DynMap to a wide-area scanning dataset and show that DynMap is capable of identifying IPs that are clearly assigned dynamically.*

Resumo. *Introduzimos o DynMap, um sistema para identificar endereços IPs alocados dinamicamente. O DynMap rastreia dispositivos utilizando assinaturas de certificados HTTPS, disponíveis publicamente, tornando-o geral e utilizável por qualquer operador. Nós avançamos o estado da arte desenvolvendo mecanismos para lidar com certificados HTTPS compartilhados por diversos dispositivos, proxies e balanceadores de carga. Nós aplicamos o DynMap num conjunto de dados e mostramos que o DynMap identifica IPs claramente dinâmicos.*

1. Introdução

O estudo de vulnerabilidades e análise forense de redes requer a identificação e rastreamento de dispositivos (*hosts*) executando serviços e aplicações. Técnicas que utilizam o endereço IP como identidade de um dispositivo assumem que endereços IP são alocados estaticamente. No entanto, a exaustão de endereços IPv4 (Richter et al. 2016) bem como a dinamicidade da alocação e virtualização de recursos em ambientes de computação em nuvem (Xiao et al. 2013) implicam em maior dinamicidade da alocação de endereços IP a múltiplos dispositivos ao longo do tempo.

Endereços IP alocados dinamicamente dificultam a análise de vulnerabilidades, adicionando ambiguidades no mapeamento de vulnerabilidades para dispositivos. Por exemplo, uma vulnerabilidade identificada em um IP dinâmico e_1 pode não ser encontrada em uma varredura (*scan*) posterior porque o serviço agora está executando no IP e_2, mesmo quando o serviço continua vulnerável. Além disso, vulnerabilidades identificadas em um IP dinâmico ao longo do tempo podem estar associadas a diferentes serviços, potencialmente não relacionados. Esse comportamento dificulta ainda mais a análise e tratamento das vulnerabilidades pelos operadores de rede, tipicamente já sobrecarregados devido à grande quantidade de vulnerabilidades que gerenciam (Tundis et al. 2018).

Nesse cenário, não existe uma base de dados consolidada de endereços IP dinâmicos que pode ser usada como referência. Apesar de existirem técnicas para classificar um IP em estático ou dinâmico, elas apresentam limitações que reduzem sua aplicabilidade. Uma técnica comum e amplamente aplicável consiste em procurar o DNS reverso (*Reverse*

DNS, RDNS) do IP que se deseja classificar e analisar o nome de domínio associado à procura de indicadores de dinamicidade (Dan et al. 2021; Fiebig et al. 2018; Nakamori et al. 2019). No entanto, muitos IPs não possuem RDNS configurado ou podem ter nomes desatualizados, fazendo com que a precisão de análises dos nomes de domínio à procura dos indicadores de dinamicidade não seja confiável (Fiebig et al. 2018). Por exemplo, apenas 30–35% dos endereços IPv4 possuem RDNS (Dan et al. 2021). Outra abordagem para identificação de IPs dinâmicos é capturar uma miríade de dados a fim de caracterizar o uso de um bloco de endereços IP (Xie et al. 2007) ou capturar o tráfego de uma rede (Jin et al. 2007). No entanto, tais dados podem ser sigilosos ou disponíveis somente em contextos específicos, por exemplo, quando os dados necessários são pertinentes a um conjunto limitado de IPs ou acessíveis somente por agentes privados. Essa dependência torna tais métodos inviáveis para contextos gerais e, por consequência, os restringem ao grupo de pesquisadores e operadores de rede que os desenvolveram ou que possuem acesso aos dados necessários.

Neste trabalho, propomos DynMap (Seção 3), um sistema para identificação de endereços IP dinâmicos a partir de dados públicos, por exemplo, os coletados por sistemas de varredura (*crawlers*) como Shodan ou Censys. O DynMap é uma extensão do UDmap, método desenvolvido pela Microsoft Research (Xie et al. 2007) que utiliza logs privados do Hotmail (Seção 2). O DynMap estende o UDmap com mecanismos que permitem a identificação de endereços IP dinâmicos utilizando assinaturas (*fingerprints*) de certificados HTTPS e chaves SSH, dados públicos que podem ser obtidos por qualquer operador e ferramentas abertas de monitoramento como o ZGrab. Os principais desafios superados pelos mecanismos propostos são (i) o tratamento de anomalias resultantes do compartilhamento de assinaturas, *e.g.,* devido ao compartilhamento de certificados e chaves, ou a presença de *proxies* HTTP reversos (Sankar et al. 2024); e (ii) a atualização de assinaturas, *e.g.,* devido à renovação de certificados HTTPS.

Caracterizamos os blocos de endereços IP dinâmicos identificados pelo DynMap, relacionando-os com metadados sobre os sistemas autônomos (ASes) que operam cada bloco (Seção 4). Nossos resultados indicam que o DynMap identifica blocos de endereços IP com perfil claramente dinâmico, utilizados primariamente por provedores de computação em nuvem, serviços de hospedagem e provedores de serviço de Internet (ISPs).

2. Fundamentos

Nosso trabalho estende o UDmap para identificar blocos de endereços IPs alocados dinamicamente utilizando dados públicos obtidos de assinaturas de certificados HTTPS e chaves SSH. A abordagem do UDmap, herdada pelo DynMap, é combinar dados sobre endereços IP para identificar *blocos contíguos* cujos endereços são alocados dinamicamente ao longo do tempo. O UDmap utiliza logs do Hotmail como entrada, em particular, o ID único de usuário é usado para rastrear usuários entre IPs. De forma simplificada, as etapas do UDmap herdadas pelo DynMap são:

Etapa 1: Seleção de Blocos Candidatos. O UDmap identifica um endereço IP como possível dinâmico caso os logs do Hotmail indiquem que ele foi utilizado por mais de um usuário. Endereços IP que não são observados nos logs, ou que foram utilizados apenas por um usuário são considerados como *lacunas*. O UDmap inicia identificando blocos de IPs que podem ser dinâmicos, denotados blocos *candidatos*. O algoritmo

constrói um bloco candidato de B IPs contíguos com três propriedades: (1) IPs em um bloco candidato devem pertencer ao mesmo AS e possuir o mesmo prefixo BGP (Marder et al. 2018), (2) um bloco candidato não pode ter lacunas com mais de L IPs consecutivos e (3) cada bloco deve possuir um mínimo de B' IPs, $B \geq B'$.

Etapa 2: Cálculo da Entropia de Uso por IP. Após construir blocos, o UDmap calcula a *entropia de uso* por IP, esse cálculo é feito bloco a bloco para os IPs naquele bloco, e captura se um usuário é observado de forma uniforme dentro de um bloco. Para cada IP em um bloco, o UDmap calcula a fração de usuários observados no IP que também foram observados em outros IPs do bloco. Uma entropia próxima de 1 indica que a maioria dos usuários aparecem na maioria dos IPs do bloco (*i.e.,* o mesmo grupo de usuários acessa o Hotmail de vários IPs diferentes), um forte indicativo de alocação dinâmica. Uma entropia próxima de zero indica que a maioria dos usuários ficam concentrados em um pequeno número de IPs, indicando baixa dinamicidade.

Etapa 3: Identificação de Sub-blocos de IP Dinâmicos. Após o cálculo da entropia para todos os IPs de todos os blocos candidatos, o UDmap refina os blocos candidatos em sub-blocos identificando seções do bloco original onde a maioria dos IPs possuem entropia acima de um limiar T. Para realizar essa classificação, o UDmap utiliza um filtro de mediana, calculado com uma janela deslizante, para suavizar variâncias bruscas transientes de entropia. Após a aplicação do filtro, o UDmap seleciona apenas os sub-blocos *contíguos* (sem lacunas) de endereços IP cuja entropia é maior que o limiar T. Os endereços IP contidos nos sub-blocos são inferidos como dinâmicos.

3. DynMap

Os logs do Hotmail são privados e o nosso objetivo é construir um sistema que possa ser aplicado em dados públicos. Para isso, precisamos encontrar um metadado que conseguimos obter de endereços IP que (1) esteja presente em uma quantidade significativa de IPs e (2) cujo valor seja único para cada dispositivo.

No DynMap, utilizamos a assinatura SHA256 de certificados X.509 recebidos de servidores HTTPS como um identificador para rastrear um serviço (Martin et al. 2016) entre diferentes endereços IP. Certificados X.509 podem ser capturados em escala global de servidores HTTPS por ferramentas como o ZGrab e estão disponíveis em sistemas de varredura como Shodan e Censys.

Porém, sítios Web precisam renovar certificados periodicamente e podem compartilhar certificados (apesar desta prática não ser recomendada). Estas ocorrências geram ambiguidades na identificação de serviços e, consequentemente, no mapeamento de serviços para os endereços IP utilizados pelos dispositivos hospedeiros.

Dinamicidade de Domínios por IP. Para contornar casos de renovação e compartilhamento de certificados HTTPS, calculamos uma segunda métrica (além da entropia de uso) para caracterizar blocos de endereços IP que chamamos *dinamicidade de domínio*, que captura se um domínio é observado de forma uniforme em múltiplas assinaturas. Para cada porta com um serviço HTTPS sondado em cada IP de um bloco, calculamos a razão entre o número de domínios e o número de assinaturas que aparecem ao longo do tempo. Se a razão é próxima de 1, todas as assinaturas possuem um domínio distinto. Neste caso, temos um mapeamento entre domínios e assinaturas: a mudança de assinatura indica que o IP é utilizado por diferentes serviços e possivelmente dinâmico (*e.g.,* servidores de um provedor

de computação em nuvem alocados a diferentes clientes ao longo do tempo). Por outro lado, se a razão é próxima de zero, então poucos domínios (possivelmente um) possuem várias assinaturas (*e.g.,* devido a mudança ou renovação de certificados); indicando que o endereço IP pode ser estático. Após calcular a razão do número de domínios e assinaturas para cada porta, selecionamos o mínimo entre todas as portas como a dinamicidade de domínio de cada endereço IP para diminuir a influência de cenários anômalos.

Análise de Comportamento. Ao plotar os histogramas da entropia de uso e dinamicidade de domínios para os IPs dos blocos candidatos, observamos que as distribuições de ambas as métricas são bimodais, isto é, as métricas indicam fortemente que os endereços IPs são estáticos ou dinâmicos. Assim, temos cinco combinações comuns de métricas que cobrem o comportamento de um endereço IP. Aplicamos as seguintes regras em cada IP no processo de inferência para combinar as duas métricas em uma única métrica final que será utilizada na etapa de identificação de sub-blocos de IPs dinâmicos:

Caso 1. Se as duas métricas são próximas de zero, então ambas as métricas indicam que o endereço IP é estático. Para estes IPs calculamos a média das duas métricas, o que resulta em uma métrica final próxima de zero.

Caso 2. Se as duas métricas são próximas de 1, então ambas as métricas indicam que o endereço IP é dinâmico. Novamente calculamos a média das duas métricas.

Caso 3. Se a entropia de uso é próxima de zero e a de dinamicidade de domínio é próxima de 1, este IP não compartilhou muitas assinaturas com outros endereços IP do bloco, mas devido à mudança de domínio na maioria ou em todas as suas portas, é provável que este IP seja dinâmico. A métrica final para o endereço IP é definida como a dinamicidade de domínios, próxima de 1.

Caso 4. Se a entropia de uso é próxima de 1 e a dinamicidade de domínio é próxima de zero, utilizamos a entropia de uso como a métrica final e estendemos a análise para refinar a inferência realizada. Calculamos as razões (i) entre o número de assinaturas do IP e a quantidade de IPs no bloco ($\mathrm{F}\frac{a}{b}$) e (ii) entre o número de domínios do IP e a quantidade de IPs no bloco ($\mathrm{F}\frac{d}{b}$). Se $\mathrm{F}\frac{a}{b}$ for menor que 0,5, temos poucas assinaturas que aparecem em muitos dos endereços IP do bloco ao longo do tempo. Nesse caso, pode ser que este endereço IP seja utilizado com um proxy reverso ou balanceador de carga, e marcamos este IP como *proxy*. Se $\mathrm{F}\frac{a}{b}$ for maior que 0,5 e $\mathrm{F}\frac{d}{b}$ for menor que 0,5, então temos muitas assinaturas e poucos domínios, indicando que uma quantidade grande de certificados é utilizada por poucos serviços. Neste caso marcamos o IP como sendo de um *servidor compartilhado* entre múltiplos serviços. Se ambas $\mathrm{F}\frac{a}{b}$ e $\mathrm{F}\frac{d}{b}$ são maiores que 0,5, temos muitos domínios e muitas assinaturas e não fazemos nenhuma classificação especial, mantendo o IP marcado simplesmente como *dinâmico*.

Caso 5. Se alguma métrica não é próxima de zero ou 1, então calculamos a métrica final como a média das duas métricas. Este IP pode ser um caso de borda (*outlier*).

Após processar os IPs de todos os blocos seguindo as regras acima e identificar os sub-blocos contíguos de IPs dinâmicos, o tipo de cada bloco é definido como o tipo prevalente entre seus IPs (*i.e.,* dinâmico, proxy e servidores compartilhados).

4. Análise e Categorização de IPs

Nesta seção apresentamos um breve sumário da parametrização do DynMap e uma caracterização de blocos dinâmicos encontrados no espaço de endereçamento da Internet brasileira para duas configurações de parâmetros.

Aplicamos o DynMap em um conjunto de dados composto de varreduras de rede realizadas pelo Shodan no espaço de endereçamento da Internet brasileira. As varreduras do Shodan cobrem endereços IP com frequência variável. Quando uma porta executando um serviço HTTPS é sondada, o Shodan coleta e exporta o certificado X.509, incluindo a assinatura SHA256 e o *common name*. Neste trabalho utilizamos o *common name* do certificado como o nome de domínio. Utilizamos os dados do Shodan coletados entre 1^{o} de outubro e 31 de dezembro de 2023. Após a extração dos dados, 14.521.920 sondagens de serviços HTTPS em 1.422.737 endereços IP distintos foram obtidas.

Não conhecemos nenhuma fonte de dados de validação (*ground truth*) para avaliação do DynMap. Operadores de rede geralmente não disponibilizam informações sobre o uso de blocos de endereços IP. Contornamos este desafio relacionando os blocos identificados como dinâmicos pelo DynMap com diversos outros conjuntos de dados que corroboram as inferências realizadas. Em particular, mapeamos os blocos para o AS que o controla utilizando a biblioteca PyASN. Estes dados nos permitem verificar se o uso do espaço de endereçamento é compatível com o tipo de rede. Também consultamos o PeeringDB para obter o tipo do AS, que é informado diretamente pelos operadores.

Escolhendo parâmetros. O DynMap possui quatro parâmetros, são eles: B o mínimo de endereços IP em um bloco candidato, L a maior lacuna permitida durante a construção de blocos candidatos, T o limiar de dinamicidade para um endereço IP ser considerado dinâmico pelo filtro de mediana durante a construção de sub-blocos e J o tamanho da janela de suavização do filtro de mediana em torno de cada endereço IP alvo.

Realizamos uma bateria de testes e identificamos que os parâmetros J e T afetam a confiabilidade das inferências. Valores altos de T tornam a construção de sub-blocos mais restritiva, classificando apenas IPs com maior métrica de dinamicidade como dinâmicos. Valores baixos de J reduzem a transferência de inferências de um IP para seus vizinhos no filtro da mediana, classificando apenas IPs que já possuem boas inferências.

Por sua vez, os parâmetros B e L afetam a cobertura das inferências, visto que impactam diretamente a construção de blocos. Valores altos de B resultam em ASes de organizações menores serem descartados, pois não têm presença suficiente no espaço de endereços para formação de blocos grandes com poucas lacunas. Valores altos de L contrapõem aumentar o valor de B, pois permitem a construção de blocos maiores flexibilizando a presença de lacunas, aumentando o número de ASes pequenos encontrados.

Categorização de IPs. Caracterizamos os IPs dinâmicos identificados para as configurações ($B = \{8, 128\}; L = 8; T = 0,5; J = 2$). A configuração com $B = 8$ identifica blocos menores contendo 144991 IPs dinâmicos de 1156 ASes, enquanto a configuração mais conservadora com $B = 128$ identifica blocos maiores contendo 36312 IPs dinâmicos de 51 ASes de maior porte. Focamos em variar o tamanho mínimo do bloco pois este é o parâmetro com maior impacto nas inferências.

A Tabela 1 mostra a quantidade de IPs dinâmicos encontrados para os 10 ASes com o maior número de IPs dinâmicos em cada configuração. A sobreposição de ASes é esperada visto que ambas as configurações identificam IPs dinâmicos em ASes grandes. Pelo nome é possível identificar que a maior parte dos ASes onde endereços IPs dinâmicos são encontrados são prestadores de serviços de hospedagem (†), computação em nuvem

Tabela 1. Sistemas autônomos com maior número de endereços IP dinâmicos identificados na Internet brasileira para duas configurações de DynMap.

Tamanho mínimo do bloco $B = 8$			Tamanho mínimo do bloco $B = 128$		
AS	Nome do AS	# de IPs	AS	Nome do AS	# de IPs
AS16509	Amazon‡	74486	AS16509	Amazon‡	8594
AS27715	Locaweb†	11932	AS27715	Locaweb†	8559
AS8075	Microsoft‡	6160	AS8075	Microsoft‡	4084
AS270631	Totvs‡	2590	AS262361	Deznet Telecom♯	1211
AS262643	BRC Telecom♯	1601	AS271229	AMX Internet♯	1024
AS262361	Deznet Telecom♯	1211	AS271453	Vitoria Networks♯	1023
AS16625	Akamai‡	1027	AS272645	Digo Internet♯	968
AS11921	Secrelnet Informatica♯	1026	AS268950	Pcsupri Informatica♯	768
AS271229	AMX Internet♯	1024	AS11921	Secrelnet Informatica♯	762
AS271453	Vitoria Networks♯	1023	AS262947	Megalynk Sistemas♯	655

Tabela 2. Tipo do AS por categoria de IP para tamanhos de bloco 8 e 128.

	$B = 8$						$B = 128$					
Tipo	Dinâmico		Proxy		Servidores		Dinâmico		Proxy		Servidores	
Empresarial	66171	86.7%	9371	12.3%	764	1.0%	3056	35.0%	5588	63.9%	98	1.1%
Conteúdo (CDN)	10726	44.2%	12227	50.3%	1340	5.5%	5108	38.2%	8019	60.0%	242	1.8%
Fibra/DSL/ISP	9590	59.2%	3123	19.3%	3485	21.5%	2298	49.4%	2350	50.6%	0	0.0%
NSP	1427	26.0%	1954	35.6%	2108	38.4%	196	32.9%	399	67.1%	0	0.0%
Educação/Pesquisa	157	65.4%	44	18.3%	39	16.2%	0	0.0%	0	0.0%	0	0.0%
Governamental	71	38.6%	73	39.7%	40	21.7%	0	0.0%	0	0.0%	0	0.0%
Serviços de rede	71	34.5%	108	52.4%	27	13.1%	0	0.0%	0	0.0%	0	0.0%
Sem fins lucrativos	3	2.5%	94	77.7%	24	19.8%	0	0.0%	0	0.0%	0	0.0%

(‡) e de acesso à Internet (♯). A prevalência de grandes empresas nos três primeiros lugares (Amazon, Locaweb, Microsoft) em ambas as execuções, demonstra que ASes de grande porte possuem muitos IPs alocados a diferentes prefixos e o DynMap foi capaz de identificar estes ASes de forma consistente.

O tipo do AS permite inferir a área de atuação da organização associada ao AS, bem como o perfil de IPs que o DynMap é capaz de encontrar. Na Tabela 2, é possível ver que a maioria dos IPs encontrados estão em redes dos tipos Empresarial, Conteúdo (CDN) e Fibra/DSL/ISP, o que alinha com o comportamento esperado de IPs dinâmicos. Ainda, com blocos maiores, a quantidade de IPs do tipo Empresarial reduziu de forma significativa, isso pode ser explicado pela redução no número de ASes menores.

5. Conclusão

Neste trabalho apresentamos DynMap, um sistema de identificação de endereços IP dinâmicos a partir de dados públicos. Nós detalhamos as mudanças e melhorias realizadas sobre o estado da arte, com foco em tratar de anomalias que provém da utilização de dados públicos que são, por natureza, variáveis e imprevisíveis. Além disso, introduzimos duas categorias de blocos de IPs, proxy e servidores compartilhados, que vão além da classificação de um IP como apenas dinâmico e enriquecem os resultados. Por fim, utilizando o DynMap, nós analisamos três meses de dados do Shodan e categorizamos os IPs encontrados, demonstrando que o nosso sistema é capaz de identificar IPs claramente dinâmicos, *e.g.,* provedores de computação em nuvem, serviços de hospedagem e ISPs, além de IPs com outros perfis de dinamicidade.

Agradecimentos

Agradecemos aos revisores da SBSeg pelos comentários. Este trabalho foi financiado pela RNP (Hackers do Bem), FAPEMIG, FAPESP, CNPq e CAPES.

Referências

Dan, Ovidiu, Vaibhav Parikh e Brian D. Davison (2021). "IP Geolocation through Reverse DNS". Em: *ACM Trans. Internet Technol.* DOI: 10.1145/3457611.

Fiebig, Tobias, Kevin Borgolte, Shuang Hao, Christopher Kruegel, Giovanni Vigna e Anja Feldmann (2018). "In rDNS We Trust: Revisiting a Common Data-Source's Reliability". Em: *Passive and Active Measurement*. Springer International Publishing. DOI: 10.1007/978-3-319-76481-8_10.

Jin, Yu, Esam Sharafuddin e Zhi Li Zhang (2007). "Identifying dynamic IP address blocks serendipitously through background scanning traffic". Em: *Proceedings of the 2007 ACM CoNEXT Conference*. Association for Computing Machinery. DOI: 10.1145/1364654.1364659.

Marder, Alexander, Matthew Luckie, Amogh Dhamdhere, Bradley Huffaker, kc claffy e Jonathan M. Smith (2018). "Pushing the Boundaries with bdrmapIT: Mapping Router Ownership at Internet Scale". Em: *Proceedings of the Internet Measurement Conference 2018*. Association for Computing Machinery. DOI: 10.1145/3278532.3278538.

Martin, Husák, Čermák Milan, Jirsík Tomáš e Čeleda Pavel (2016). "HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting". Em: *EURASIP Journal on Information Security*. DOI: 10.1186/s13635-016-0030-7.

Nakamori, Tomofumi, Daiki Chiba, Mitsuaki Akiyama e Shigeki Goto (2019). "Detecting Dynamic IP Addresses and Cloud Blocks Using the Sequential Characteristics of PTR Records". Em: *Journal of Information Processing*. DOI: 10.2197/ipsjjip.27.525.

Richter, Philipp, Georgios Smaragdakis, David Plonka e Arthur Berger (2016). "Beyond Counting: New Perspectives on the Active IPv4 Address Space". Em: *Proceedings of the Internet Measurement Conference 2016*. Association for Computing Machinery. DOI: 10.1145/2987443.2987473.

Sankar, Vedha, Varsha Bharanikumar e Lakshmi Swaminathan (2024). "Dynamic Load Balancing and Resource Optimization Algorithm for Reverse Proxy Servers". Em: *2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS)*. DOI: 10.1109/ICC-ROBINS60238.2024.10533888.

Tundis, Andrea, Wojciech Mazurczyk e Max Mühlhäuser (2018). "A review of network vulnerabilities scanning tools: types, capabilities and functioning". Em: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. Association for Computing Machinery. DOI: 10.1145/3230833.3233287.

Xiao, Zhen, Weijia Song e Qi Chen (2013). "Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment". Em: *IEEE Transactions on Parallel and Distributed Systems*. DOI: 10.1109/TPDS.2012.283.

Xie, Yinglian, Fang Yu, Kannan Achan, Eliot Gillum, Moises Goldszmidt e Ted Wobber (2007). "How Dynamic are IP Addresses?" Em: *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. Association for Computing Machinery. DOI: 10.1145/1282380.1282415.